

REMARKS

Claim Rejections - 35 USC §103

At page 6, claims 1, 3-4, 6, 8, 9, 11, 12, 14, 17-23, and 25 are rejected under 35 USC §103(a) as unpatentable over US patent application publication 2002/0147920, Mauro in view of US patent application publication 2002/0150243, Craft, et al (hereinafter Craft).

With respect to claim 1, it is asserted that Mauro discloses a method for managing cryptographic keys that are specific to a personal device, including retrieving in a secure processing point separated from and arranged in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device, the secure processing point storing a data package in the personal device, the data package including at least one cryptographic key.

The Office further asserts that Mauro does not disclose receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the chip; associating the unique chip identifier with the received backup data package; and storing the backup data package and the associated unique chip identifier in a permanent public database.

The following remarks are in addition to those previously presented in applicant's response of May 17, 2007. Specifically with respect to Mauro, the Office states at page 5, lines 17-20:

"Examiner is interpreting Figures 2 and 3 of Mauro to have the 'Secure processing point' separated from an[d] arranged in communication with personal device because the figure clearly shows the secure point being separated from the personal device by a bus system (allowing them to be in communication)".

Such a statement appears to be at variance to the very description presented in Mauro regarding Figures 2 and 3. Specifically, with respect to Figure 2 it is stated at paragraphs [0017] and [0018]:

“FIG. 2 is a block diagram of an embodiment of a remote terminal capable of implementing various aspects of the invention;”.

“FIG. 3 is a diagram of a specific embodiment of a secure unit within the remote terminal.”

It is therefore abundantly clear that the elements shown in Figures 2 and 3 all reside in a signal device, namely a remote terminal 110, and it is therefore not seen how the secure unit 240 shown in Figures 2 and 3 of Mauro is separated from and in communication with the remote terminal (personal device) when it is in fact part of the remote terminal. Bus 232 is simply the means for interconnecting the various modules of the remote terminal 110. As clearly seen in Figure 2, remote terminal 110 is directed to all of the elements shown and not just to the elements to the left of bus 232.

In this regard, the Office in the “Response to Arguments” section at page 2 of the Official Action, in response to applicant’s arguments of May 17, 2007, asserts that the present application at page 8, lines 9-30, only states that the secure processing point 150 and the personal device are in communication, but does not recite two separate devices communicating to each other. This assertion is believed to be at variance with the overall specification and accompanying drawings of the present application.

Specifically with respect to Figure 1, page 8, lines 1-3 state that it exemplifies a system which includes the elements and illustrates the operation of preferred embodiments of the invention. Further at page 8, lines 9-15 make clear that the personal device is separate from the secure processing point because the secure processing point is used during the assembly of the device.

Figure 2 of the present application is an illustration showing possible device management activities that can be performed “after shipment of the device assembled in FIG. 1” (page 8, lines 5-6, emphasis added). If the device is assembled in Figure 1, clearly

the secure processing point is not part of the personal device, but is simply used during its assembly as clearly explained in the specification of the present application. The secure processing point is therefore “separated from” the personal device as set forth in claim 1.

Consequently, the claimed action as set forth in claim 1 of retrieving in a secure processing point separated from and arranged in communication with the personal device requires two separate devices, contrary to the position asserted by the Office while, what is shown in Figures 2 and 3 of Mauro, clearly represents a single device, namely a remote terminal. Therefore, this feature of claim 1 is not disclosed in Mauro.

As stated above, the Office relies on Craft with respect to the last three actions recited in claim 1, including “receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret key stored in a tamper-resistant secret storage of the chip”. The Office asserts that this is shown in Craft by “A server system receives encrypted content data using permanent, hardware-embedded cryptographic keys (tamper-resistant secret storage) from a client.” Reliance is made to paragraphs [0019] and [0021] of Craft directed to the Description of the Drawings section. However, paragraph [0019] only describes that there is a data processing system for secure communication of application code and content using permanent, hardware-embedded cryptographic keys. This paragraph does not state anything about what is sent from the client (personal device) to the server (secure processing point) and *vice versa*.

Paragraph [0021] is also in the “Description of the Drawings” section of Craft and recites therein, “...a process by which a server system with knowledge of the required server private key receives and authenticates a request for encrypted application code and/or encrypted content data from a client...”. This statement in Craft only indicates that the server receives a request for code and/or data from the client. As is evident in the “Summary of Invention” section of Craft, Craft merely discloses that a) a client sends an encrypted message to a server, which message requests some content; then b) the server decrypts the request message and authenticates the client; and finally c) the server encrypts

the requested content and sends it to the client. This overall operation of Craft is described in detail in its various embodiments, including the embodiment described at paragraphs [0047]-[0050] which details the encryption/decryption process that is generally referred to with respect to the flow chart shown in Figure 4 as described in paragraph [0021].

However, what is recited in claim 1 is directed to a backup function; namely, the receiving at the secure processing point, in response to storing the data package in the personal device, a backup data package from the personal device where this backup data package is the data package that the personal device received, but encrypted with the unique secret chip key stored in a tamper-resistant secret store of the chip (the chip being an integrated circuit chip included in the personal device).

However, such an action is in no way suggested by Craft since Craft is directed to the server decrypting a request message from the client, where the request is for application code and/or content data, the request having embedded therein a client serial number and encrypted client authentication data which the server then uses to authenticate the client. In response to such authentication, the server transmits the requested application code and/or content data to the client. The backup function of the present invention, if it were to be implied by Craft, would necessarily correspond to sending back the application code and/or content data that was requested by the client from the server, back to the server with encryption thereof by the client. Such a backup is not disclosed or suggested by Craft. In fact, the disclosure in Craft ends with the transmitting of the application code and/or content to the client in an encrypted form (see Figure 5, step 518 and accompanying description at paragraphs [0051]-[0054]).

The secure processing point of the present invention receiving an encrypted backup data package which is encrypted with the unique secret chip key of the personal device, has a particular purpose in the present invention which, in fact, is the storing of the backup data package and the associated unique chip identifier in a permanent public database, which effectively makes retrieval thereof straightforward for the personal device if, for some reason, the stored data package in the personal device is corrupted or lost for some reason.

In Craft, no such purpose is indicated and it would appear rather confusing and totally superfluous to encrypt the application code and/or content at the client and return it back to the server since this would serve no purpose for the server. In short, why would the server need the same application code and/or content data that it has delivered to the client sent back to the server in an encrypted form? In Craft, if the client later experiences a malfunction with respect to the downloaded content or if the downloaded application code and/or content data is lost, the client can simply repeat the request to the server as shown in Figures 3 and 4 thereof, which provides the client with the same application data and/or content data that it had previously received.

In the above comments, it should be noted that the term “unique secret chip key” as used in claim 1 is being considered as being analogous to the “client private key” 218 as shown in Figure 2 of Craft. However, this client private key 218 in Craft is only used for encrypting the client authentication data as disclosed, for example, at paragraph [0048] of Craft. The client authentication data is retrieved by the server from the client in response to the request message before any application data and/or content data is sent to the client.

As defined in claim 1 of the present application, the unique secret chip key is used by the personal device for encrypting the data package after the data package has been stored in the personal device for purposes of generating a backup data package. Such a use of the client private key 218 in Craft is not disclosed or suggested.

With respect to the action recited in claim 1 of associating the unique chip identifier with the received backup data package, this feature is also not disclosed in Craft. In particular, since there is no backup data package generated in Craft, this action is simply not disclosed in Craft. Indeed, at paragraph [0041] of Craft, it discloses a “unique client serial number”, which could be interpreted as including the term “unique chip identifier”. However, the client serial number is not associated with any backup data package in Craft. Instead, at paragraph [0051], Craft states that it is included in the client request message and is used to search for an associated client public key by the server.

Finally, the last action of claim 1 is the storing of the backup data package and the associated unique chip identifier in a permanent public database. There is no such operation performed in Craft. Indeed, the client serial number as evidenced by paragraph [0043] of Craft is associated with a client public key and stored in a public database. However, the client public key is not a backup data package as explained above and it is not a data package that has been stored in and received from the personal device with encryption by a unique secret chip key.

In short, the reliance on paragraph [0043] is believed to be inappropriate since that deals only with the manufacture of the client CPU chip where the client serial number and client public key, corresponding to the client private key 218 in the client device, are associatively retained for subsequent use by storing in a client public key data store. Such storage of the client serial number and client public key corresponding to the client private key has nothing to do with a personal device having a data package stored therein by a secure processing point, with the data package including at least one cryptographic key, and the personal device in response to receiving the data package generating a backup data package which is encrypted with a unique secret chip key stored in a tamper-resistant secret storage of a chip in the personal device.

In short, the retrieving of application data and/or content data by a client in Craft in response to a request message has nothing to do with receiving a data package, including at least one cryptographic key, as required by claim 1. The storage in a client public key data store 222 of a client serial number and a client public key corresponding to a client private key, has nothing to do with a backup data package from a personal device in response to the personal device receiving such a data package from a secure processing point.

In summary, the features of claim 1 that the Office states are disclosed in Craft, but not in Mauro, are in fact not disclosed in Craft, and the combining of Craft with Mauro would not provide to a person of ordinary skill in the art the necessary information to suggest claim 1.

It is therefore respectfully submitted that claim 1 is not suggested by the cited art and reconsideration of the rejection of claim 1 is earnestly solicited.

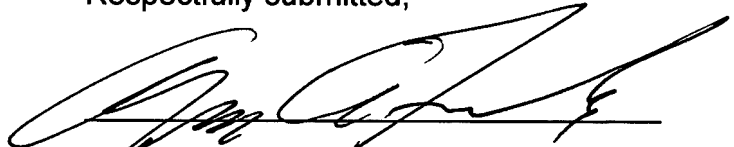
Independent system claim 9, independent personal device claim 18, and independent secure processing point claim 25 all recite features corresponding to those set forth in claim 1 and, for similar reasons, each of these independent claims is also believed to be distinguished over Mauro in view of Craft.

Since each of the independent claims is believed to be distinguished over the cited art, it is respectfully submitted that all of the dependent claims are further distinguished over the cited art due to their dependency from an independent claim which is believed to be distinguished over the art.

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance and reconsideration of the claim rejections is earnestly solicited.

The undersigned respectfully submits that no fee is due for filing this Response. The Commissioner is hereby authorized to charge to deposit account 23-0442 any fee deficiency required to submit this paper.

Respectfully submitted,



Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550

Dated: September 24, 2007

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955